



COMMUNITY DAY

AOTEAROA



COMMUNITY DAY

AOTEAROA



Reducing your AWS Compliance Workload

Chamila de Alwis
Senior Cloud Architect, APN Ambassador
Leaven





COMMUNITY DAY

AOTEAROA

Compliance?



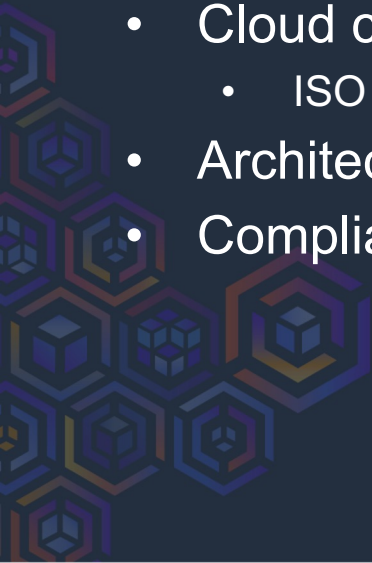


COMMUNITY DAY

AOTEAROA

Compliance Landscape

- Guidelines around control objectives and activities
- Cloud considerations for industry standards
 - ISO 27017
- Architects vs Compliance
- Compliance tracking and auditing in the Cloud





COMMUNITY DAY

AOTEAROA

Compliance Landscape

- Industry Standards
 - ISO27001
 - PCI DSS etc
- Country specific regulation
 - New Zealand – NZISM
 - USA – NIST SP 800-100
- Government specific Cloud Risk Assessment workbooks
- Organization specific controls
- Client specific controls





COMMUNITY DAY

AOTEAROA

Compliance for the Cloud





COMMUNITY DAY

AOTEAROA

Security OF the Cloud

- Responsibility – CSP
- Concerns
 - Datacenter security
 - Physical device security
 - Hardware and software segregation between tenants
 - Availability

Security IN the Cloud

- Responsibility – CSC
- Concerns
 - Secure architecture
 - Secure configuration
 - Technical best practices
 - Infrastructure-as-Code
 - Version controlling, code reviews
 - Static code analysis
 - Change management process and a defined path to production

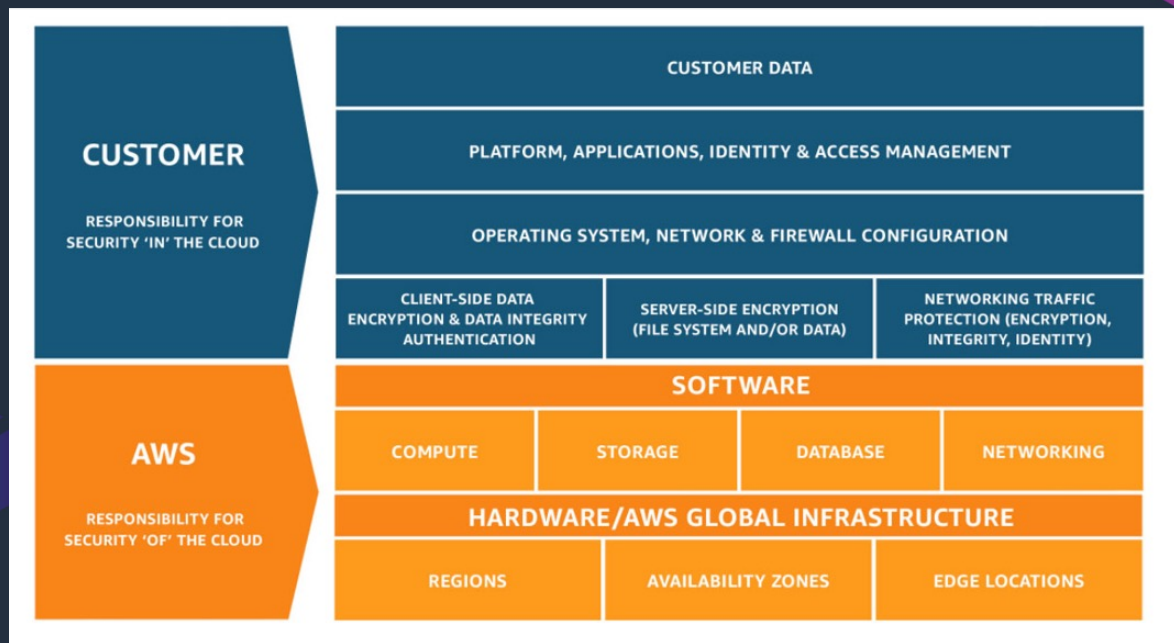




COMMUNITY DAY

AOTEAROA

Shared Responsibility Model





COMMUNITY DAY

AOTEAROA



AWS Artifact



Agreements

Reports

Documentation

FAQ

Forum

AWS reports (114) [Info](#)

Copy report URL

Download report

Q soc 21 matches

< 1 > ⚙

	Title	Reporting period	Category	Description
				Scroll down to the bottom of the page to copy, print, or download the report. To download the report, scroll down to the bottom of the page to download it.
<input type="radio"/>	System and Organization Controls (SOC) 1 Report - Previous (Apr 1 2022 - Sep 30 2022)	April 1, 2022 to September 30, 2022	Certifications and Attestations	This document evaluates the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICFR). The audit is performed according to the SSAE 18 and ISAE 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley efforts.
<input type="radio"/>	System and Organization Controls (SOC) 1 Report - Previous (Oct 1 2021 - Mar 31 2022)	October 1, 2021 to March 31, 2022	Certifications and Attestations	This document evaluates the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICFR). The audit is performed according to the SSAE 18 and ISAE 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley efforts.
<input type="radio"/>	System and Organization Controls (SOC) 1 Report - Previous (Spanish) (Apr 1 2022 - Sep 30 2022)	April 1, 2022 to September 30, 2022	Certifications and Attestations	This document evaluates the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICFR). The audit is performed according to the SSAE 18 and ISAE 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley efforts. The SOC report was originally prepared in English by EY, and the opinion is based on the System Description and the service auditor's tests of controls as presented in English. The Spanish language report has been prepared by AWS for informational purposes only.
<input type="radio"/>	System and Organization Controls (SOC) 2 Privacy Report - Previous (Apr 1 2022 - Sep 30 2022)	April 1, 2022 to September 30, 2022	Certifications and Attestations	This document evaluates the AWS controls that meet the criteria for privacy in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria.
<input type="radio"/>	System and Organization Controls (SOC) 2 Report - Current (Oct 1 2022 - Mar 31 2023)	October 1, 2022 to March 31, 2023	Certifications and Attestations	The AWS SOC 2 Type 2 report evaluates the AWS controls that meet the criteria for security, availability, confidentiality, and privacy in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria. This is our most recent SOC 2 report. SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits twice a year over a period of 6 months – Oct 1-Mar 31 and Apr 1-Sept 30. Once the audit period is over, our auditors prepare their audit report which is then released in May and November, respectively. Should you seek assurance that we have maintained the control environment described in this most recent SOC report, we make a SOC Continued Operations Letter available to you in Artifact. Scroll down to the bottom of the page to download it.
<input type="radio"/>	System and Organization Controls (SOC) 2 Report - Previous (Apr 1 2022 - Sep 30 2022)	April 1, 2022 to September 30, 2022	Certifications and Attestations	This document evaluates the AWS controls that meet the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria.
<input type="radio"/>	System and Organization Controls (SOC) 2 Report - Previous (Oct 1 2021 - Mar 31 2022)	October 1, 2021 to March 31, 2022	Certifications and Attestations	This document evaluates the AWS controls that meet the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria.



COMMUNITY DAY



AWS Compliance Center Overview

Resources

CONTENTS

- Regulations
- Resources

Country-specific | General | Compliance Programs

Using AWS in the Context of New Zealand Privacy Considerations

This document provides information to assist customers who want to use AWS to store or process content containing personal information, in the context of key privacy considerations and the New Zealand Privacy Act 1993 ("Privacy Act"). It will help customers understand: The way AWS services operate, including how customers can address security and encrypt their content. The geographic locations where customers can choose to store content and other relevant considerations. The respective roles the customer and AWS each play in managing and securing content stored on AWS services.

AWS Workbook for the Reserve Bank of New Zealand Guidance

The Reserve Bank of New Zealand (RBNZ) Guidance on Cyber Resilience Workbook covers the domains and practices within the RBNZ's Guidance on Cyber Resilience. Where applicable, the workbook provides supporting details and references to assist organizations in managing their workloads on AWS.









AWS Compliance Center Overview

Resources

CONTENTS

- Regulations
- Resources

Country-specific | General | Compliance Programs

 cloud security alliance	 International Organization for Standardization	 International Organization for Standardization	 International Organization for Standardization
CSA	ISO 9001	ISO 27001	ISO 27017
 International Organization for Standardization	 GDPR	 PARTICIPATING ORGANIZATION™	 AICPA SOC Accounting and Auditing Councils International
ISO 27018	GDPR	PCI DSS Level 1	SOC

AWS Compliance Center Overview

New Zealand

CONTENTS

- Regulations
- Resources

Regulations

Can financial institutions use AWS? ⊖

Who is the financial regulator? ⊖

What regulations apply to financial institutions using AWS? ⊖

Key considerations for financial institutions using AWS ⊖

Achieving Compliance in AWS

Use AWS Config! Thank you!

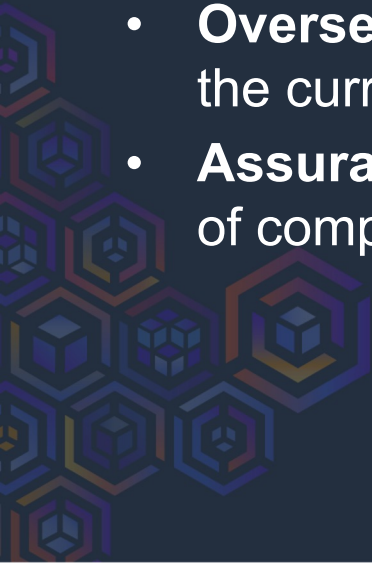


COMMUNITY DAY

AOTEAROA

Three Lines Model

- **Manage risks** – define baseline controls
- **Oversee risks** – single pane of glass view of the current status of controls
- **Assurance** – ability to be audited, to provide evidence of compliance





COMMUNITY DAY

AOTEAROA

Manage Risks





COMMUNITY DAY

AOTEAROA

Maintain a Baseline Configuration

- Move fast, don't break anything
- Preventive and Detective Controls
- AWS Config
 - Firewall Rules
 - Backup Policies
 - IaC - CFN Guard, Checkov Rules
 - SCPs, Permission Boundaries
- Control Tower





COMMUNITY DAY

AOTEAROA

Oversee Status





COMMUNITY DAY

AOTEAROA

Single Pane of Glass View

- AWS Config
 - Conformance Packs
- Security Hub
 - Frameworks





AWS Config ✕

- Dashboard
- Conformance packs
- Rules
- Resources**
- Aggregators
 - Conformance packs
 - Rules
 - Resources
 - Authorizations
- Advanced queries
- Settings

- What's new [🔗](#)
- Documentation [🔗](#)
- Partners [🔗](#)
- FAQs [🔗](#)
- Pricing [🔗](#)
- Share feedback [🔗](#)

AWS Config > Resources > vol-[REDACTED] > Timeline

Timeline

General details

Resource ID

vol-[REDACTED]

Resource type

AWS::EC2::Volume

Resource name

-

Events

All times are in Pacific/Auckland (UTC+12:00)

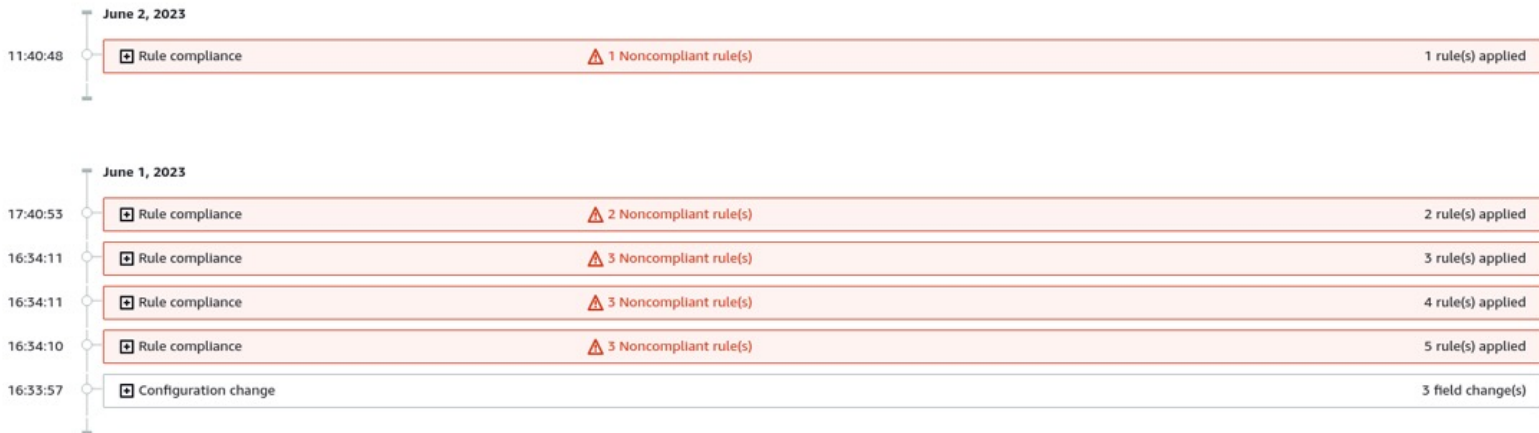
Start date

2023/06/06

Now

Event type

All event types





COMMUNITY DAY

AOTEAROA

Provide Assurance





COMMUNITY DAY

AOTEAROA

Auditors Come Knocking

- Endless Days of Screenshots and Excel Sheets
 - Aggregate evidence instead of single resources
 - Journey instead of single point in time
- Audit (+InfoSec) vs Architect gap
 - Short term orbital view of a solution from Auditors
 - Long term "indoctrinated" tunnel vision from engineering
- Automate as much as possible
 - AWS Audit Manager!!!





AWS Audit Manager > Dashboard

Dashboard [Info](#)

Last updated: November 19, 2021, 9:25 PM UTC

Filter by

All active assessme... ▼

Create assessment

Daily snapshot [Info](#)

Controls with non-compliant evidence

⚠ 308

Non-compliant evidence

⚠ 796

Active assessments

6
....

Controls with non-compliant evidence grouped by control domain [Info](#)

You can view up to 10 controls for each domain. If you applied an assessment filter, you can download a .csv file to view all controls for a domain.

Control domain

Evidence breakdown

▼ Identity and access management (10 of 169)

8.2.4.a For a sample of system components, inspect system configuration settings to verify that user ...





COMMUNITY DAY

AOTEAROA



Identity and access management (10 of 169)

8.2.4.a For a sample of system components, inspect system configuration settings to verify that user ...	
8.2.3.a For a sample of system components, inspect system configuration settings to verify that user ...	
16.9 - Disable Dormant Accounts	
8.2 To verify that users are authenticated using unique ID and additional authentication ...	
8.2.3.b Additional testing procedure for service provider assessments only: Review internal processes ...	
8.2.5.b Additional testing procedure for service provider assessments only: Review internal processes ...	
8.2.5.a For a sample of system components, obtain and inspect system configuration settings to verify...	
8.2.4.b Additional testing procedure for service provider assessments only: Review internal processes ...	
AC-2(1) Account Management Automated System Account Management	
AC-2.j.1 Account Management	

Evidence breakdown

	Non-compliant	18
	Compliant	0
	Inconclusive	4

SOC 2

Standard

SOC 2 is an auditing procedure that ensures a company's data is securely managed protecting the interests of the organization and privacy of clients.

40 manual controls
21 automated controls

SOC 2



NIST SP 800-171 Rev. 2

Standard

NIST SP 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, and recommends specific security requirements to achieve that objective. NIST 800-171 is a publication that outlines the required security standards and practices for non-federal organizations that handle CUI on their networks.





COMMUNITY DAY

AOTEAROA

Bridging the Gap



Auditors

- AWS Audit Academy
 - Beginner
 - Advanced
 - Domain Specific
- Public AWS resources
 - Ex: NZISM implementation guide
- Overall Cloud Awareness
 - Shared Responsibility Model (and nuances)
 - Elasticity in the Cloud
 - Focus on Security IN the Cloud



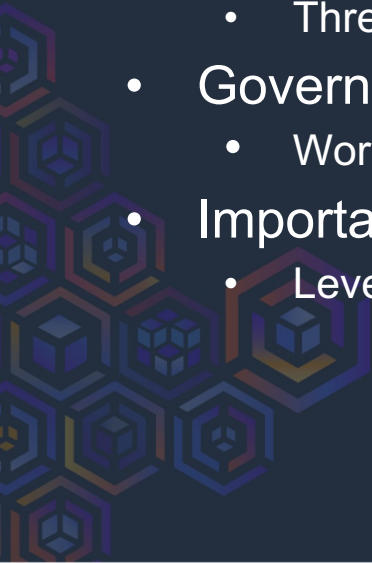


COMMUNITY DAY

AOTEAROA

Architects

- Risk oriented approach for architecting
 - Three Lines Model
- Governance for risk management
 - Work with Info Sec team
- Importance of Process Controls
 - Leverage organizational controls





COMMUNITY DAY

AOTEAROA

Recap

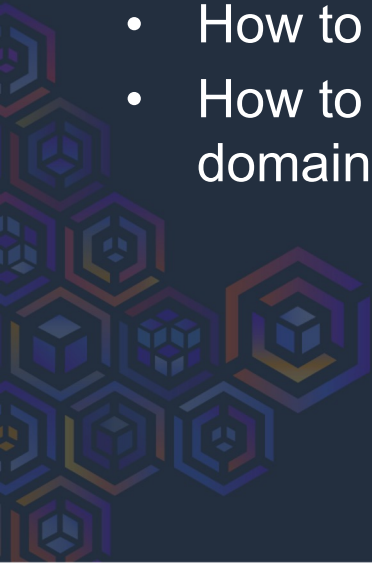




COMMUNITY DAY

AOTEAROA

- What Compliance in AWS solutions look like
- How to target for a compliant architecture
- How to bridge the gap between seemingly separate domains





COMMUNITY DAY

AOTEAROA

Thank You!





COMMUNITY DAY

AOTEAROA